FIG.1

TRANSMISSION NODE — 101

RELAY NODE — 102

RADIO NODE — 103

RADIO SECTION

IEEE1394 BUS — 104

FIG.2

~ 406

MPEG
STORAGE UNIT

MPEG VIDEO

~ 403

COPY PROTECTION
PROCESSING UNIT

AUTHENTICATION
FORMAT (DEVICE
CERTIFICATE) Acert

KEY K

~ 405

ENCRYPTION UNIT

[MPEG VIDEO]K

~ 402

AV/C PROTOCOL
PROCESSING UNIT

~ 404

ISO SIGNAL
TRANSMISSION &
RECEPTION UNIT

~ 401

IEEE1394 I/F

receive authentication request device certificate

APPROVED
BY
DRAFTSMAN

O.G. FIG.
CLASS SUBCLASS

ET # 0039-7378-29 SHEET 3 OF 68

3/68

FIG.3

RADIO NODE CONTROL PACKET TRANSMISSION & RECEPTION UNIT — 211

RADIO SECTION CONFIGURATION RECOGNITION UNIT — 209

RADIO ISO SIGNAL TRANSMISSION & RECEPTION UNIT — 205

RADIO I/F — 202

RADIO SECTION

COPY PROTECTION CONTROL/FORWARD UNIT — 210

PROXY SUB-UNIT CONFIGURATION UNIT — 207

PROXY TABLE — 208

ISO SIGNAL TRANSMISSION & RECEPTION UNIT — 204

1394 BUS CONFIGURATION RECOGNITION UNIT — 206

AV/C PROTOCOL PROCESSING UNIT — 203

IEEE1394 I/F — 201

IEEE1394 BUS

FIG.4

307 DISPLAY UNIT

VIDEO

306 MPEG DECODING UNIT

MPEG VIDEO

303 COPY PROTECTION PROCESSING UNIT

AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Acert

KEY K

305 DECRYPTION UNIT

[MPEG VIDEO]K

302 RADIO NODE CONTROL PACKET TRANSMISSION & RECEPTION UNIT

304 RADIO ISO SIGNAL TRANSMISSION & RECEPTION UNIT

301 RADIO I/F

FIG.5

TRANSMISSION NODE 101   RELAY NODE 102   RADIO NODE 103

RADIO NODE CONFIGURATION INFORMATION — S501

PROXY INFORMATION GENERATION & ADVERTISEMENT TO 1394 BUS SIDE — S502

AV/C
(TRANSMITTING STREAM TO MPEG DECODING/DISPLAY SUB-UNIT & SETTING UP ISOCHRONOUS CHANNEL #x) — S503

SETTING UP BOTH INTERNAL ISO SIGNAL TRANSMISSION & RECEPTION UNITS — S504

RADIO NODE CONTROL PACKET
(TRANSMITTING ISO SIGNAL THROUGH RADIO ISOCHRONOUS CHANNEL #y) — S505

[MPEG VIDEO]k
(THROUGH ISOCHRONOUS CHANNEL #x) — S506

[MPEG VIDEO]k
(THROUGH RADIO ISOCHRONOUS CHANNEL #y) — S507

AUTHENTICATION TARGET QUERY
FROM;RADIO NODE,(MPEG DECODING/DISPLAY SUB-UNIT,ID=0),(CH=#y) — S521

AUTHENTICATION TARGET REPLY
FROM;RELAY NODE,(VIDEO TRANSMISSION SUB-UNIT,ID=0),(CH=#y) — S522

AUTHENTICATION REQUEST
TO:RELAY NODE,(VIDEO TRANSMISSION SUB-UNIT,ID=0),Bcert — S508

AUTHENTICATION TARGET QUERY
FROM;RELAY NODE,(MPEG DECODING/DISPLAY SUB-UNIT,ID=0),CH=#x — S523

AUTHENTICATION TARGET REPLY
FROM;TRANSMISSION NODE,(VIDEO TRANSMISSION SUB-UNIT,ID=0),CH=#x — S524

AUTHENTICATION REQUEST
TO:TRANSMISSION NODE:(VIDEO TRANSMISSION SUB-UNIT,ID=0),Bcert — S509

6/68

FIG.6

COPYRIGHT: (illegible)

TRANSMISSION NODE 101　　　RELAY NODE 102　　　RADIO NODE 103

AUTHENTICATION REQUEST
TO:RELAY NODE:(MPEG DECODING/DISPLAY SUB-UNIT:ID=0),Acert,Bdid
S510

AUTHENTICATION REQUEST
TO:RADIO NODE :
(MPEG DECODING/DISPLAY SUB-UNIT:ID=0),Acert,Bdid
S511

AUTHENTICATION & KEY EXCHANGE PROCEDURE
TO:RELAY NODE,(VIDEO TRANSMISSION SUB-UNIT,ID=0)
S512

AUTHENTICATION &
KEY EXCHANGE PROCEDURE
TO:TRANSMISSION NODE :
(VIDEO TRANSMISSION SUB-UNIT:ID=0)
S513

AUTHENTICATION & KEY EXCHANGE PROCEDURE
TO:RADIO NODE,(MPEG DECODING/DISPLAY SUB-UNIT:ID=0)
S515

AUTHENTICATION &
KEY EXCHANGE PROCEDURE
TO:RELAY NODE :
(MPEG DECODING/DISPLAY SUB-UNIT:ID=0)
S514

EXCHANGE KEY & SEED TRANSFER
TO:RADIO NODE :
(MPEG DECODING/DISPLAY SUB-UNIT:ID=0)
S519

EXCHANGE KEY & SEED TRANSFER
TO:RELAY NODE :
(MPEG DECODING/DISPLAY SUB-UNIT:ID=0)
S516

[MPEG VIDEO]K(THROUGH RADIO ISOCHRONOUS CHANNEL #y)
S517

[MPEG VIDEO]K
(THROUGH ISOCHRONOUS CHANNEL #x)
S518

FIG.7

START

S601

RECOGNIZE THAT MPEG DECODING/DISPLAY SUB-UNIT EXISTS IN RELAY NODE 102 (S502)

S602

ESTABLISH ISOCHRONOUS CHANNEL #x ON 1394 BUS USING AV/C PROTOCOL & SEND COMMAND "CONNECT THIS TO THE ABOVE SUB-UNIT & DISPLAY" TO RELAY NODE 102 (S503)

S603

SEND ENCRYPTED MPEG VIDEO THROUGH ISOCHRONOUS CHANNEL #x (S506)

S631

RECEIVE AUTHENTICATION TARGET QUERY. STORE DESTINATION NODE, SUB-UNIT, ETC. OF #x, & NOTIFY SUB-UNIT THAT IS TRANSMITTING DATA TO #x, TO RELAY NODE (S523,S524)

S604

RECEIVE AUTHENTICATION REQUEST (S509) (INTERPRETED AS BEING RECEIVED FROM MPEG DECODING/DISPLAY SUB-UNIT OF RELAY NODE)

S605

OBTAIN B'S AUTHENTICATION FORMAT (DEVICE CERTIFICATE) (Bcert) & EXTRACT Bdid, ETC.

S606

SEND OWN AUTHENTICATION FORMAT (DEVICE CERTIFICATE) (Acert), ETC. TO MPEG DECODING/DISPLAY SUB-UNIT OF RELAY NODE ALONG WITH Bdid (S510)

S607

RECEIVE PACKET 513 (INTERPRETED AS BEING RECEIVED FROM MPEG DECODING/DISPLAY SUB-UNIT OF RELAY NODE)

S608

CHECK TAMPERING, CHECK Bcert & CALCULATE AUTHENTICATION KEY Kauth

R1

FIG.8

R1

TRANSMIT AUTHENTICATION & KEY EXCHANGE PROCEDURE 514 TO MPEG DECODING/DISPLAY SUB-UNIT OF RELAY NODE — S609

ENCRYPT MPEG VIDEO BY USING KEY K — S610

TRANSMIT ENCRYPTED MPEG VIDEO [MPEG VIDEO]K THROUGH ISOCHRONOUS CHANNEL #x (S518) — S611

FIG.9

START

S701

RECEIVE RADIO NODE CONFIGURATION INFORMATION (S501) (CONFIRM THAT RADIO NODE HAS AUTHENTICATION FORMAT)

S702

PROXY CONFIGURATION OF RADIO NODE CONFIGURATION (SUB-UNIT INFORMATION) AS OWN SUB-UNIT (OF RELAY NODE). REGISTER CORRESPONDENCE INTO PROXY TABLE (S502)

S703

ADVERTISE THE ABOVE PROXY SUB-UNIT CONFIGURATION TO EXTERNAL (THROUGH IEEE1212 REGISTER, AV/C PROTOCOL, ETC.) (ADVERTISED AS ONE THAT HAS AUTHENTICATION FORMAT) (S502)

S704

RECEIVE AV/C COMMAND (S503) (INPUT STREAM FROM ISOCHRONOUS CHANNEL #x INTO MPEG DECODING/DISPLAY SUB-UNIT)

S705

CHECK NODE TO WHICH AV/C COMMAND SHOULD BE ACTUALLY ISSUED BY REFERRING TO PROXY TABLE

S706

RESERVE ISOCHRONOUS CHANNEL #y OF RADIO SECTION

R2

FIG.10

R2

S707

CONNECT ISO SIGNAL TRANSMISSION & RECEPTION UNIT (THAT RECEIVES ISOCHRONOUS CHANNEL #x) 204 WITH RADIO ISO SIGNAL TRANSMISSION & RECEPTION UNIT (THAT TRANSMITS ISOCHRONOUS CHANNEL #y)205. MAKE IT POSSIBLE TO OUTPUT INPUT SIGNAL FROM 1394 I/F TO RADIO SECTION (S504)

S708

NOTIFY DATA TRANSMISSION, TO RADIO NODE THROUGH RADIO ISOCHRONOUS CHANNEL #y (S505)

S709

FORWARD SIGNAL TRANSMITTED FROM TRANSMISSION NODE THROUGH ISOCHRONOUS CHANNEL #x, TO ISOCHRONOUS CHANNEL #y OF RADIO SECTION (S506,S507)

S731

RECEIVE AUTHENTICATION QUERY. STORE DESTINATION NODE, SUB-UNIT, ETC. OF #y & NOTIFY SUB-UNIT THAT IS TRANSMITTING DATA TO #y, TO RADIO NODE (S521,S522)

S710

RECEIVE AUTHENTICATION REQUEST (WISH TO CARRY OUT AUTHENTICATION PROCEDURE WITH VIDEO TRANSMISSION SUB-UNIT) FROM RADIO NODE (S508)

S732

SEND AUTHENTICATION TARGET QUERY TO TRANSMISSION NODE IN ORDER TO INQUIRE SUB-UNIT THAT IS TRANSMITTING DATA TO #x. AT THAT POINT, ALSO NOTIFY SUB-UNIT THAT RECEIVES DATA THROUGH #x (S523), & OBTAIN REPLY (S524)

R3

11/68

FIG.11

R3

S711
FORWARD THE ABOVE AUTHENTICATION REQUEST TO TRANSMISSION NODE 101 WITHOUT CHANGING CONTENTS, BY REFERRING TO PROXY TABLE 208 (S509)

S712
RECEIVE AUTHENTICATION REQUEST 510 (WISH TO CARRY OUT AUTHENTICATION PROCEDURE WITH MPEG DECODING/DISPLAY SUB-UNIT) FROM TRANSMISSION NODE

S713
FORWARD THE ABOVE AUTHENTICATION REQUEST TO RADIO NODE 103 WITHOUT CHANGING CONTENTS, BY REFERRING TO PROXY TABLE 208 (S511)

S714
FORWARD AUTHENTICATION & KEY EXCHANGE PROCEDURE PACKET 512 FROM RADIO NODE 103, TO TRANSMISSION NODE 101 WITHOUT CHANGING CONTENTS (S513)

S715
FORWARD AUTHENTICATION PROCEDURE PACKET 514, EXCHANGE KEY, ETC. FROM TRANSMISSION NODE 101, TO RADIO NODE 103 WITHOUT CHANGING CONTENTS (S515,519)

S716
FORWARD ENCRYPTED MPEG VIDEO THAT IS TRANSMITTED FROM TRANSMISSION NODE THROUGH ISOCHRONOUS CHANNEL #x (S516), TO RADIO NODE 103 THROUGH RADIO CHANNEL #y WITHOUT CHANGING CONTENTS (S517)

FIG.12

```
        ┌──────────────┐
        │    START     │
        └──────────────┘
               │
               ▼                                    S801
┌─────────────────────────────────────────────────────┐
│ TRANSMIT RADIO NODE CONFIGURATION                     │
│ INFORMATION (S501) (NOTIFY THAT MPEG                  │
│ DECODING/DISPLAY FUNCTION EXISTS) (ALSO NOTIFY        │
│ THAT RADIO NODE HAS AUTHENTICATION FORMAT)            │
└─────────────────────────────────────────────────────┘
               │                                    S802
               ▼
┌─────────────────────────────────────────────────────┐
│ RECEIVE RADIO NODE CONTROL PACKET (S505)              │
│ (THAT DATA WILL BE TRANSMITTED THROUGH                │
│ RADIO ISOCHRONOUS CHANNEL #y IS NOTIFIED)             │
└─────────────────────────────────────────────────────┘
               │                                    S803
               ▼
┌─────────────────────────────────────────────────────┐
│ RECEIVE ENCRYPTED DATA FROM RADIO                     │
│ ISOCHRONOUS CHANNEL #y (S507)                         │
└─────────────────────────────────────────────────────┘
               │                                    S831
               ▼
┌─────────────────────────────────────────────────────┐
│ SEND AUTHENTICATION TARGET QUERY TO RELAY             │
│ NODE IN ORDER TO INQUIRE SUB-UNIT THAT IS             │
│ TRANSMITTING DATA TO #y. AT THAT POINT. ALSO          │
│ NOTIFY SUB-UNIT THAT RECEIVES DATA THROUGH            │
│ #y (S521), & OBTAIN REPLY (S522)                      │
└─────────────────────────────────────────────────────┘
               │                                    S804
               ▼
┌─────────────────────────────────────────────────────┐
│ TRANSMIT AUTHENTICATION REQUEST TO                    │
│ RELAY NODE (S508)                                     │
└─────────────────────────────────────────────────────┘
               │                                    S805
               ▼
┌─────────────────────────────────────────────────────┐
│ RECEIVE AUTHENTICATION REQUEST 511 (WISH TO           │
│ CARRY OUT AUTHENTICATION PROCEDURE WITH               │
│ MPEG DECODING/DISPLAY FUNCTION) (SOURCE BEING         │
│ INTERPRETED AS RELAY NODE 102)                        │
└─────────────────────────────────────────────────────┘
               │                                    S806
               ▼
┌─────────────────────────────────────────────────────┐
│ TRANSMIT AUTHENTICATION & KEY EXCHANGE                │
│ PROCEDURE PACKET 512 TO RELAY NODE (S512)             │
└─────────────────────────────────────────────────────┘
               │
               ▼
            ┌──────┐
            │  R4  │
            └──────┘
```

FIG.13

R4

↓

S807

RECEIVE AUTHENTICATION & KEY EXCHANGE PROCEDURE PACKET 515 (SOURCE BEING INTERPRETED AS RELAY NODE 102)

↓

S808

CHECK TAMPERING, CHECK Acert & CALCULATE AUTHENTICATION KEY Kauth

↓

S809

RECEIVE ENCRYPTED MPEG VIDEO THROUGH RADIO ISOCHRONOUS CHANNEL #y (S519)

↓

S810

DECRYPT IT BY USING CONTENTS KEY K & EXTRACT MPEG VIDEO

↓

S811

MPEG DECODING AT MPEG DECODING UNIT

↓

S812

VIDEO DISPLAY AT DISPLAY UNIT

14/68

FIG.14

DESTINATION NODE = RELAY NODE
SOURCE NODE = RADIO NODE
CONFIGURATION-1 = MPEG DECODING/DISPLAY FUNCTION
CONFIGURATION-2 = · · · · · ·
⋮
ATTRIBUTE-1 OF CONFIGURATION-1 = AUTHENTICATION FORMAT (AUTHENTICATION ORGANIZATION = · · · · · ·)
ATTRIBUTE-2 OF CONFIGURATION-1 = MPEG UPPERBOUND BIT RATE 6Mbps
⋮

FIG.15

SUBSTANCE ON RADIO SECTION SIDE	FORM OF PROXY SERVICE PROVIDED BY RELAY NODE WITH RESPECT TO 1394 SIDE
MPEG DECODING/DISPLAY FUNCTION OF RADIO NODE 103 (SUB-UNIT ID=0) (AUTHENTICATION FORMAT) IS PRESENT	MPEG DECODING/DISPLAY SUB-UNIT (SUB-UNIT ID=0) (AUTHENTICATION FORMAT) IS PRESENT

FIG.16

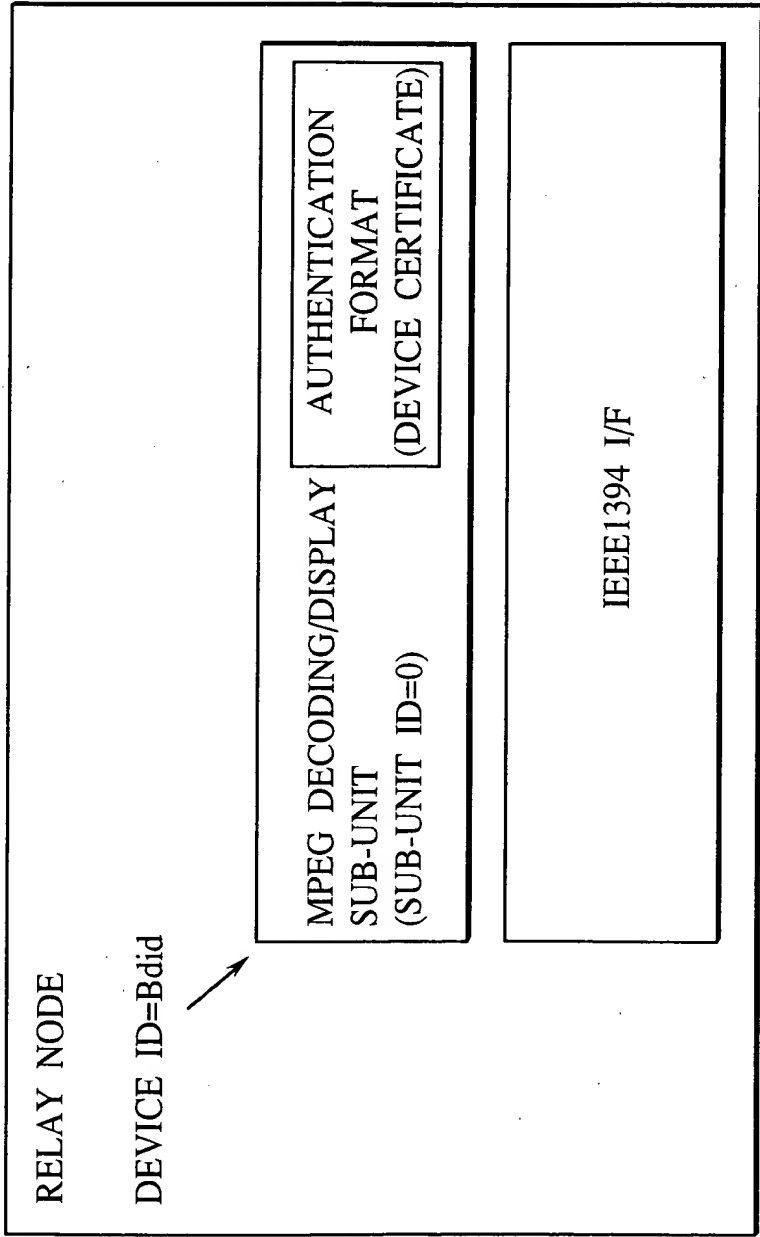| SUBSTANCE ON 1394 BUS SIDE	FORM OF PROXY SERVICE PROVIDED BY RELAY NODE WITH RESPECT TO RADIO SECTION SIDE
VIDEO TRANSMISSION FUNCTION OF TRANSMISSION NODE 101 (VIDEO TRANSMISSION SUB-UNIT) (SUB-UNIT ID=0) (AUTHENTICATION FORMAT) IS PRESENT	VIDEO TRANSMISSION SUB-UNIT (SUB-UNIT ID=0) (AUTHENTICATION FORMAT) IS PRESENT
------	----------

FIG.17

RELAY NODE

DEVICE ID=Bdid

MPEG DECODING/DISPLAY SUB-UNIT (SUB-UNIT ID=0)

AUTHENTICATION FORMAT (DEVICE CERTIFICATE)

IEEE1394 I/F

FIG.18

RELAY NODE

DEVICE ID=Adid

VIDEO TRANSMISSION SUB-UNIT (SUB-UNIT ID=0)	AUTHENTICATION FORMAT (DEVICE CERTIFICATE)
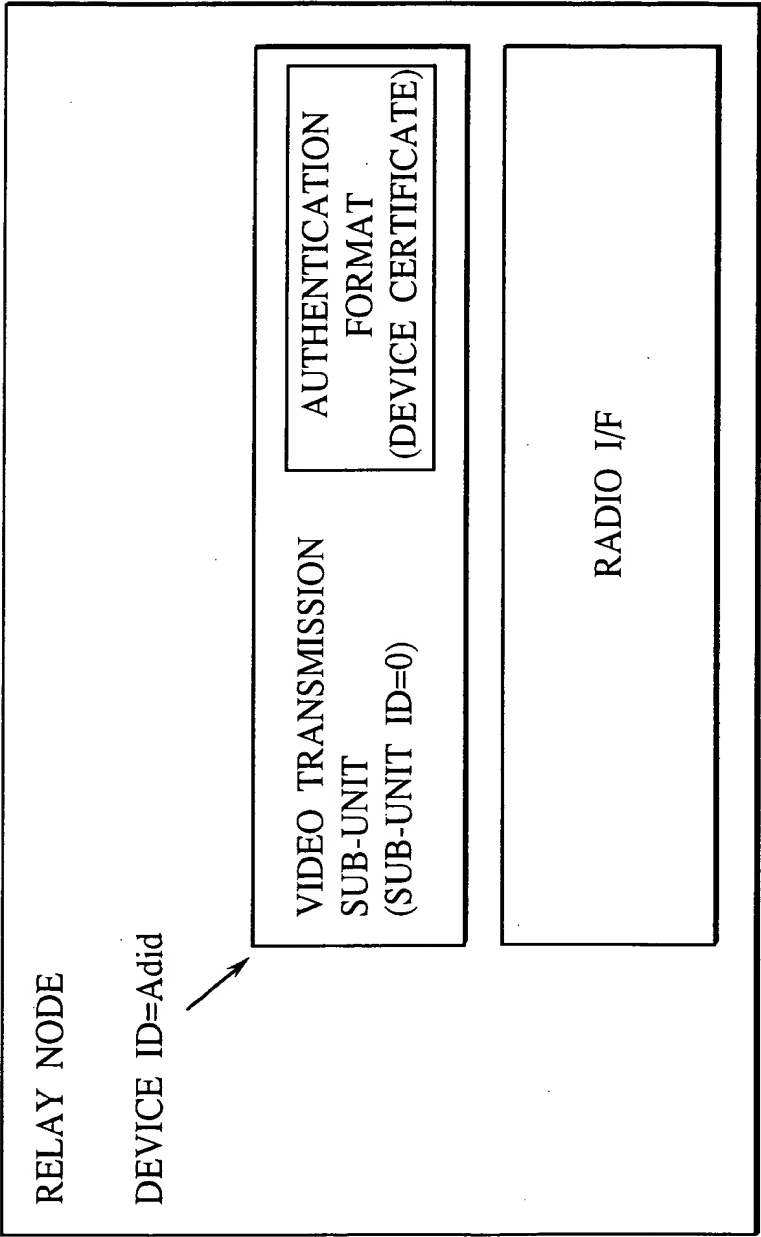
RADIO I/F

FIG.19

DESTINATION NODE = RADIO NODE

SOURCE NODE = RELAY NODE

CONTROL CONTENT = DATA RECEPTION

RADIO ISOCHRONOUS CHANNEL TO BE USED = #y

DATA DESTINATION =
MPEG DECODING/DISPLAY FUNCTION (ID=0)

DATA SOURCE =
VIDEO TRANSMISSION FUNCTION (ID=0)

FIG.20

RADIO NODE ⟋2103

RADIO SECTION

RELAY NODE ⟋2102

IEEE1394 BUS

2104

TRANSMISSION NODE ⟋2101

FIG.21

FIG.22

- 2211 RADIO SECTION CONFIGURATION RECOGNITION UNIT
- 2212 RADIO SECTION COPY PROTECTION PROCESSING UNIT — AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Ccert
- 2213 RADIO NODE CONTROL PACKET TRANSMISSION & RECEPTION UNIT
- 2202
- RADIO I/F
- RADIO NETWORK
- 2210 PROXY SUB-UNIT CONFIGURATION UNIT
- 2214 PROXY TABLE
- 2205 ENCRYPTION UNIT
- KEY K2
- [MPEG VIDEO] K2
- 2206 RADIO ISO SIGNAL TRANSMISSION & RECEPTION UNIT
- MPEG VIDEO
- 2204 DECRYPTION UNIT
- 2203 ISO SIGNAL TRANSMISSION & RECEPTION UNIT
- 2201
- 2209 1394 BUS CONFIGURATION RECOGNITION UNIT
- 2208 IEEE 1394 COPY PROTECTION PROCESSING UNIT — AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Bcert
- KEY K1
- [MPEG VIDEO] K1
- 2207 AV/C PROTOCOL PROCESSING UNIT
- IEEE1394 I/F
- IEEE1394 BUS

FIG.23

```
                                              ┌──────────────────┐  ~2307
                                              │   DISPLAY UNIT   │
                                              └──────────────────┘
                                                       ▲
                                                       │ VIDEO
                                              ┌──────────────────┐  ~2306
                                              │      MPEG        │
                                              │  DECODING UNIT   │
                                              └──────────────────┘
                                                       ▲
                                                       │ MPEG VIDEO
┌─────────────────────────┐ ~2303                      │
│ COPY PROTECTION         │                            │
│ PROCESSING UNIT         │        KEY K      ┌──────────────────┐  ~2305
│  ┌────────────────────┐ │ ───────────────▶  │ DECRYPTION UNIT  │
│  │ AUTHENTICATION     │ │                   └──────────────────┘
│  │ FORMAT (DEVICE     │ │                            ▲
│  │ CERTIFICATE) Dcert │ │                            │ [MPEG VIDEO]K
│  └────────────────────┘ │                            │
└─────────────────────────┘                            │
           │                              ┌──────────────────────┐ ~2304
┌─────────────────────────┐ ~2302        │ RADIO ISO SIGNAL     │
│ RADIO NODE              │               │ TRANSMISSION &       │
│ CONTROL PACKET          │               │ RECEPTION UNIT       │
│ TRANSMISSION &          │               └──────────────────────┘
│ RECEPTION UNIT          │                            ▲
└─────────────────────────┘                            │
           │                                           │       ~2301
┌──────────────────────────────────────────────────────────────┐
│                         RADIO I/F                              │
└──────────────────────────────────────────────────────────────┘
```

FIG.24

TRANSMISSION NODE 2101   RELAY NODE 2102   RADIO NODE 2103

RADIO NODE CONFIGURATION INFORMATION — S2501

PROXY INFORMATION GENERATION & ADVERTISEMENT TO 1394 BUS SIDE — S2502

AV/C (TRANSMITTING STREAM TO MPEG DECODING/DISPLAY SUB-UNIT & SETTING UP ISOCHRONOUS CHANNEL #x) — S2503

SETTING UP BOTH INTERNAL ISO SIGNAL TRANSMISSION & RECEPTION UNITS — S2504

RADIO NODE CONTROL PACKET (TRANSMITTING ISO SIGNAL THROUGH RADIO) — S2505

[MPEG VIDEO]K1(VIA #x) — S2506

AUTHENTICATION TARGET QUERY FROM;RELAY NODE,(MPEG DECODING/DISPLAY SUB-UNIT,ID=0),(CH=#x) — S2507

AUTHENTICATION TARGET REPLY FROM;TRANSMISSION NODE,(VIDEO TRANSMISSION SUB-UNIT,ID=0),(CH=#x) — S2508

AUTHENTICATION REQUEST TO:TRANSMISSION NODE:(VIDEO TRANSMISSION SUB-UNIT:ID=0),Bcert — S2509

AUTHENTICATION REQUEST TO:RELAY NODE:(MPEG DECODING/DISPLAY SUB-UNIT:ID=0),Acert,Bdid — S2510

AUTHENTICATION & KEY EXCHANGE PROCEDURE — S25111

S25112

EXCHANGE KEY & SEED TRANSFER — S2512

[MPEG VIDEO]K1(VIA #x) — S2513

S2506

DECRYPTION — S2514

MPEG VIDEO — S2515

RE-ENCRYPTION — S2516

[MPEG VIDEO]K2 (FROM;RELAY NODE,TO:RADIO NODE,SID= α) — S2517

FIG.25

TRANSMISSION NODE 2101   RELAY NODE 2102   RADIO NODE 2103

AUTHENTICATION TARGET QUERY
FROM;RADIO NODE,
(MPEG DECODING/DISPLAY SUB-UNIT,ID=0),(SID=α)   S2518

AUTHENTICATION TARGET REPLY
FROM;RELAY NODE,
(VIDEO TRANSMISSION SUB-UNIT,ID=0),(SID=α)   S2519

AUTHENTICATION REQUEST
TO:RELAY NODE,
(VIDEO TRANSMISSION SUB-UNIT:ID=0),Bcert   S2520

AUTHENTICATION REQUEST
TO:RADIO NODE,
(MPEG DECODING/DISPLAY SUB-UNIT:ID=0),Acert,Bdid   S2521

AUTHENTICATION & KEY EXCHANGE PROCEDURE   S2522 S2523

EXCHANGE KEY & SEED TRANSFER   S2524

[MPEG VIDEO]K1(VIA #x)   S2525

DECRYPTION   S2526
MPEG VIDEO   S2527
RE-ENCRYPTION   S2528
[MPEG VIDEO]K2
(FROM;RELAY NODE,
TO:RADIO NODE,SID=α)   S2529

DECRYPTION   S2530

FIG.26

START

S2601

RECOGNIZE THAT MPEG DECODING/DISPLAY SUB-UNIT EXISTS IN RELAY NODE 2102

S2602

ESTABLISH ISOCHRONOUS CHANNEL #x ON 1394 BUS USING AV/C PROTOCOL & SEND COMMAND "CONNECT THIS TO THE ABOVE SUB-UNIT & DISPLAY" TO RELAY NODE 2102

S2603

SEND ENCRYPTED MPEG VIDEO THROUGH ISOCHRONOUS CHANNEL #x (CONTENTS KEY = K1)

S2604

RECEIVE AUTHENTICATION TARGET QUERY (CHANNEL #x) FROM (MPEG DECODING/DISPLAY SUB-UNIT OF) RELAY NODE

S2605

SEARCH TRANSMISSION SUB-UNIT OF CHANNEL #x & RETURN "AUTHENTICATION TARGET IS VIDEO TRANSMISSION SUB-UNIT" AS AUTHENTICATION TARGET REPLY TO RELAY NODE

S2606

RECEIVE AUTHENTICATION REQUEST FOR VIDEO TRANSMISSION SUB-UNIT

S2607

OBTAIN B'S AUTHENTICATION FORMAT (DEVICE CERTIFICATE) (Bcert)

R5

27/68

FIG.27

(R5)

S2608

SEND OWN AUTHENTICATION FORMAT
(DEVICE CERTIFICATE) Acert, ETC.
(OF VIDEO TRANSMISSION SUB-UNIT) AS
AUTHENTICATION REQUEST, TO MPEG
DECODING/DISPLAY SUB-UNIT OF RELAY NODE

S2609

AUTHENTICATION & KEY EXCHANGE PROCEDURE
(CALCULATE AUTHENTICATION KEY Kauth1)

S2610

TRANSFER EXCHANGE KEY & SEED TO RELAY NODE

S2611

ENCRYPT MPEG VIDEO BY USING CONTENTS KEY K1

S2612

SEND ENCRYPTED MPEG VIDEO THROUGH
ISOCHRONOUS CHANNEL #x

FIG.28

START

S2701

RECEIVE RADIO NODE CONFIGURATION INFORMATION
(CONFIRM THAT RADIO NODE HAS AUTHENTICATION
FORMAT)

S2702

PROXY CONFIGURATION OF RADIO NODE
CONFIGURATION (SUB-UNIT INFORMATION) AS OWN
SUB-UNIT (OF RELAY NODE).
REGISTER CORRESPONDENCE INTO PROXY TABLE

S2703

ADVERTISE THE ABOVE PROXY SUB-UNIT
CONFIGURATION TO EXTERNAL (THROUGH IEEE1212
REGISTER, AV/C PROTOCOL, ETC.) (ADVERTISED AS
ONE THAT HAS AUTHENTICATION FORMAT)

S2704

RECEIVE AV/C COMMAND (INPUT STREAM FROM
ISOCHRONOUS CHANNEL #x INTO MPEG
DECODING/DISPLAY SUB-UNIT)

S2705

REFER TO PROXY TABLE

S2706

RESERVE QOS OF RADIO SECTION

S2707

CONNECT ISO SIGNAL TRANSMISSION & RECEPTION
UNIT (THAT RECEIVES ISOCHRONOUS CHANNEL #x)2203
WITH RADIO ISO SIGNAL TRANSMISSION & RECEPTION
UNIT 2206. MAKE IT POSSIBLE TO OUTPUT INPUT
SIGNAL FROM 1394 I/F TO RADIO SECTION

S2708

TRANSMIT RADIO NODE CONTROL PACKET TO
RADIO NODE

R6

FIG.29

(R6)

S2709
RECEIVE DATA TRANSMITTED FROM TRANSMISSION NODE THROUGH ISOCHRONOUS CHANNEL #x & RECOGNIZE THAT IT IS ENCRYPTED DATA

S2710
SEND AUTHENTICATION TARGET QUERY TO TRANSMISSION NODE THAT IS SOURCE OF DATA IN ORDER TO INQUIRE TRANSMISSION SUB-UNIT (ALSO NOTIFY THAT RECEIVING SUB-UNIT IS MPEG DECODING/DISPLAY SUB-UNIT AT THE SAME TIME.) ALSO SEND ISOCHRONOUS CHANNEL NUMBER #x

S2711
RECEIVE AUTHENTICATION TARGET REPLY FROM TRANSMISSION NODE. THE FACT THAT TRANSMISSION SUB-UNIT IS VIDEO TRANSMISSION SUB-UNIT IS ASCERTAINED

S2712
SEND AUTHENTICATION REQUEST TO VIDEO TRANSMISSION SUB-UNIT OF TRANSMISSION NODE (ALSO SEND AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Bcert OF MPEG DECODING/DISPLAY SUB-UNIT)

S2713
RECEIVE AUTHENTICATION REQUEST FOR MPEG DECODING/DISPLAY SUB-UNIT

S2714
OBTAIN AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Acert OF VIDEO TRANSMISSION SUB-UNIT OF TRANSMISSION NODE

S2715
AUTHENTICATION & KEY EXCHANGE PROCEDURE (CALCULATE AUTHENTICATION KEY Kauth1)

S2716
RECEIVE EXCHANGE KEY & SEED FROM TRANSMISSION NODE

(R7)

FIG.30

(R7)

S2717
CALCULATE CONTENTS KEY K1

S2718
RECEIVE ENCRYPTED MPEG VIDEO THROUGH ISOCHRONOUS CHANNEL #x & DECRYPT IT

S2719
RE-ENCRYPT THAT MPEG DATA BY USING CONTENTS KEY K2

S2720
SEND ENCRYPTED MPEG VIDEO BY ASSIGNING SID= α USING RADIO FRAME

S2721
RECEIVE AUTHENTICATION TARGET QUERY FROM (MPEG DECODING/DISPLAY SUB-UNIT OF) RADIO NODE (SID= α)

S2722
SEARCH TRANSMISSION SUB-UNIT OF SID= α & RETURN "AUTHENTICATION TARGET IS VIDEO TRANSMISSION SUB-UNIT" AS AUTHENTICATION TARGET REPLY TO RADIO NODE

S2723
RECEIVE AUTHENTICATION REQUEST FOR VIDEO TRANSMISSION SUB-UNIT

S2724
OBTAIN D'S AUTHENTICATION FORMAT (DEVICE CERTIFICATE) (Dcert)

S2725
SEND OWN AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Ccert, ETC.
(OF VIDEO TRANSMISSION SUB-UNIT) AS AUTHENTICATION REQUEST TO MPEG DECODING/DISPLAY SUB-UNIT OF RADIO NODE

(R21)

31/68

FIG.31

(R21)

S2726
AUTHENTICATION & KEY EXCHANGE PROCEDURE
(CALCULATE AUTHENTICATION KEY Kauth2)

S2727
TRANSFER EXCHANGE KEY & SEED TO RADIO NODE

S2728
ENCRYPT MPEG VIDEO BY USING CONTENTS KEY K2

S2729
SEND ENCRYPTED MPEG VIDEO BY ASSIGNING SID= α

FIG.32

```
( START )
```

S2801

TRANSMIT RADIO NODE CONFIGURATION
INFORMATION (NOTIFY THAT MPEG
DECODING/DISPLAY SUB-UNIT EXISTS & CONFIRM
THAT RADIO NODE HAS AUTHENTICATION FORMAT)

S2802

RECEIVE RADIO NODE CONTROL PACKET

S2803

RECEIVE ENCRYPTED MPEG VIDEO TO WHICH SID= α
IS ASSIGNED, USING RADIO FRAME

S2804

TRANSMIT AUTHENTICATION TARGET QUERY FROM
MPEG DECODING/DISPLAY SUB-UNIT TO RELAY
NODE (SID= α)

S2805

RECEIVE "AUTHENTICATION TARGET IS VIDEO
TRANSMISSION SUB-UNIT" AS AUTHENTICATION
TARGET REPLY

S2806

TRANSMIT AUTHENTICATION REQUEST FOR VIDEO
TRANSMISSION SUB-UNIT
(CONTAINING AUTHENTICATION FORMAT (DEVICE
CERTIFICATE) Dcert)

S2807

RECEIVE AUTHENTICATION REQUEST FOR MPEG
DECODING/DISPLAY SUB-UNIT CONTAINING
AUTHENTICATION FORMAT (DEVICE CERTIFICATE)
Ccert, ETC. OF VIDEO TRANSMISSION SUB-UNIT OF
RELAY NODE

(R8)

FIG.33

R8

↓ S2808

AUTHENTICATION & KEY EXCHANGE PROCEDURE
(CALCULATE AUTHENTICATION KEY Kauth2)

↓ S2809

RECEIVE EXCHANGE KEY & SEED FROM RELAY NODE

↓ S2810

CALCULATE CONTENTS KEY K2

↓ S2811

DECRYPT ENCRYPTED MPEG VIDEO THAT HAS BEEN
TRANSMITTED WITH SID=α ASSIGNED

↓ S2812

MPEG DECODING & VIDEO DISPLAY AT DISPLAY UNIT

FIG.34

SUBSTANCE ON RADIO SECTION SIDE	FORM OF PROXY SERVICE PROVIDED BY RELAY NODE WITH RESPECT TO 1394 SIDE
MPEG DECODING/DISPLAY FUNCTION OF RADIO NODE 103 (SUB-UNIT ID=0)	MPEG DECODING/DISPLAY SUB-UNIT (SUB-UNIT ID=0)

FIG.35

SUBSTANCE ON 1394 BUS SIDE	FORM OF PROXY SERVICE PROVIDED BY RELAY NODE WITH RESPECT TO RADIO SECTION SIDE
VIDEO TRANSMISSION FUNCTION OF TRANSMISSION NODE 101 (VIDEO TRANSMISSION SUB-UNIT) (SUB-UNIT ID=0)	VIDEO TRANSMISSION SUB-UNIT (SUB-UNIT ID=0)
------	----------

FIG.36

RELAY NODE

MPEG DECODING/DISPLAY SUB-UNIT (SUB-UNIT ID=0)

AUTHENTICATION FORMAT (DEVICE CERTIFICATE)

IEEE1394 I/F

FIG.37

RELAY NODE

VIDEO TRANSMISSION SUB-UNIT (SUB-UNIT ID=0)

AUTHENTICATION FORMAT (DEVICE CERTIFICATE)

RADIO I/F

FIG.38

SOURCE ADDRESS
DESTINATION ADDRESS
DATA

FIG.39

DESTINATION NODE = RADIO NODE
SOURCE NODE = RELAY NODE
CONTROL CONTENT = DATA RECEPTION
SID TO BE USED = α
DATA DESTINATION = MPEG DECODING/DISPLAY SUB-UNIT (SUB-UNIT ID=0)
DATA SOURCE = VIDEO TRANSMISSION SUB-UNIT (SUB-UNIT ID=0)

FIG.40

6103 — RECEPTION NODE

INTERNET/TELEPHONE NETWORK

6105

6102 — HOME GATEWAY

6101 — TRANSMISSION NODE

IEEE1394 BUS

6104

41/68

FIG.41

```
                                              ┌─────────────────┐ ～6406
                                              │      MPEG       │
                                              │  STORAGE  UNIT  │
                                              └─────────────────┘
                                                       ║
                                                       ║ MPEG  VIDEO
                                                       ▼
    ┌──────────────────────────┐ ～6403
    │ COPY   PROTECTION        │
    │ PROCESSING   UNIT        │
    │  ┌────────────────────┐  │         ┌─────────────────┐ ～6405
    │  │ AUTHENTICATION     │  │ KEY  K  │                 │
    │  │ FORMAT (DEVICE     │──┼────────▶│ ENCRYPTION UNIT │
    │  │ CERTIFICATE) Acert │  │         │                 │
    │  └────────────────────┘  │         └─────────────────┘
    └──────────────────────────┘                  ║
              │                                    ║ [MPEG  VIDEO]K
              │                                    ▼
    ┌──────────────────────┐ ～6402       ┌───────────────────────┐ ～6404
    │ AV/C  PROTOCOL       │              │ ISO  SIGNAL           │
    │ PROCESSING   UNIT    │              │ TRANSMISSION  &       │
    │                      │              │ RECEPTION   UNIT      │
    └──────────────────────┘              └───────────────────────┘
              │                                    ║
              │                                    ║ ～6401
    ┌─────────┴──────────────────────────────────▼─────────────────┐
    │                    IEEE1394  I/F                              │
    └───────────────────────────────────────────────────────────────┘
```

FIG.42

6209 — 1394 BUS CONFIGURATION RECOGNITION UNIT

6211 — HOME PAGE CREATION & STORAGE UNIT

6210 — PROXY HOME PAGE CREATION UNIT

6215 — CONVERSION TABLE

6214 — MPEG2/MPEG4 CONVERSION UNIT

6212 — INTERNET SIDE COPY PROTECTION PROCESSING UNIT

AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Ccert

6213 — CONTROL PACKET TRANSMISSION & RECEPTION UNIT

6205 — ENCRYPTION UNIT

KEY K2

MPEG4 VIDEO

[MPEG4 VIDEO]K2

6206 — AV SIGNAL TRANSMISSION & RECEPTION UNIT

6202 — INTERNET I/F

INTERNET

6204 — DECRYPTION UNIT

KEY K1

MPEG2 VIDEO

6208 — IEEE 1394 COPY PROTECTION PROCESSING UNIT

AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Bcert

6203 — ISO SIGNAL TRANSMISSION & RECEPTION UNIT

[MPEG2 VIDEO]K1

6207 — AV/C PROTOCOL PROCESSING UNIT

6201 — IEEE1394 I/F

IEEE1394 BUS

FIG.43

```
                                              ┌──────────────────┐  ～6307
                                              │  DISPLAY  UNIT   │
                                              └──────────────────┘
                                                      ↑
                                                    VIDEO
                                              ┌──────────────────┐  ～6306
                                              │     MPEG4        │
                                              │  DECODING  UNIT  │
                                              └──────────────────┘
                                                      ↑
                                                 MPEG4  VIDEO
┌────────────────────────────┐ ～6303
│ COPY  PROTECTION           │          ┌──────────────────┐  ～6305
│ PROCESSING  UNIT           │ KEY  K   │ DECRYPTION  UNIT │
│ ┌────────────────────────┐ │ ──────→  └──────────────────┘
│ │ AUTHENTICATION         │ │                  ↑
│ │ FORMAT (DEVICE         │ │          [MPEG4  VIDEO]K
│ │ CERTIFICATE) Bcert     │ │          ┌──────────────────┐  ～6304
│ └────────────────────────┘ │          │ AV  SIGNAL       │
└────────────────────────────┘          │ TRANSMISSION  &  │
┌────────────────────┐ ～6302           │ RECEPTION  UNIT  │
│ CONTROL  PACKET    │                  └──────────────────┘
│ TRANSMISSION  &    │                          ↑
│ RECEPTION  UNIT    │                          ↑
└────────────────────┘                          │
          │                                      │  ～6301
┌──────────────────────────────────────────────────────┐
│                  INTERNET  I/F                         │
└──────────────────────────────────────────────────────┘
```

FIG.44

TRANSMISSION NODE 6101

HOME GATEWAY 6102
(IP ADDRESS=C)

RECEPTION NODE 6103
(IP ADDRESS=D)

CONFIGURATION RECOGNITION
(READING IEEE1212 REGISTER) — S6501
PANEL — S6502

CREATING HOME PAGE FOR
TRANSMISSION NODE CONTROL — S6503

SENDING HOME PAGE — S6504

VIDEO TRANSMISSION REQUEST, SESSION CONTROL
(DECIDING TO USE FLOW ID (C,c,D,d)) — S6505

AV/C
(ISOCHRONOUS CHANNEL #x SET UP,
VIDEO TRANSMISSION REQUEST) — S6506

[MPEG2 VIDEO]K1 (VIA #x) — S6507

AUTHENTICATION TARGET QUERY
(FROM;HOME GATEWAY, MPEG DECODING/DISPLAY SUB-UNIT,ID=0),(CH=#x) — S6508

AUTHENTICATION TARGET REPLY
(FROM;TRANSMISSION NODE, VIDEO TRANSMISSION SUB-UNIT,ID=0),(CH=#x) — S6509

AUTHENTICATION REQUEST
(TO:TRANSMISSION NODE: VIDEO TRANSMISSION SUB-UNIT:ID=0),Bcert — S6510

AUTHENTICATION REQUEST
(TO:HOME GATEWAY NODE: MPEG DECODING/DISPLAY SUB-UNIT:ID=0),Acert,Bdid — S6511

AUTHENTICATION & KEY EXCHANGE
PROCEDURE — S6512

Kauth1 SHARING — S6513

Kauth1 SHARING
EXCHANGE KEY & SEED TRANSFER — S6514

K1 CALCULATION

[MPEG2 VIDEO]K1(VIA #x) — S6515

DECRYPTION USING K1 — S6516
— S6517
MPEG2 VIDEO
MPEG2/MPEG4 CONVERSION — S6518
MPEG4 VIDEO — S6519
RE-ENCRYPTION — S6520
— S6521

[MPEG VIDEO]K2
(FROM;HOME GATEWAY,
TO:RECEPTION NODE,
FLOW ID=(C,c,D,d))

FIG.45

TRANSMISSION NODE 6101

HOME GATEWAY 6102
(IP ADDRESS=C)

RECEPTION NODE 6103
(IP ADDRESS=D)

AUTHENTICATION REQUEST
(TO:HOMEGATEWAY, AUTHENTICATION PORT),
FLOW ID=(C,c,D,d) S6522

AUTHENTICATION REQUEST
(TO:RECEPTION NODE, AUTHENTICATION PORT),
FLOW ID=(C,c,D,d) S6523

AUTHENTICATION & KEY EXCHANGE
PROCEDURE
FLOW ID=(C,c,D,d) S6524

S6525

Kauth2 SHARING

Kauth2 SHARING

EXCHANGE KEY & SEED TRANSFER
FLOW ID=(C,c,D,d) S6526

[MPEG2 VIDEO]K1(VIA #x)
S6527

S6528 DECRYPTION USING K1

S6529 MPEG2 VIDEO

S6530 MPEG2/MPEG4 CONVERSION

S6531 MPEG4 VIDEO

S6532 RE-ENCRYPTION

S6533 [MPEG VIDEO]K2
(FROM;HOME GATEWAY,TO:RECEPTION NODE),
FLOW ID=(C,c,D,d)

S6534 DECRYPTION

FIG.46

START

S6601

IEEE1212 REGISTER IS READ FROM
HOME GATEWAY 6102

S6602

TRANSMISSION OF PANEL SUB-UNIT IS REQUESTED
FROM HOME GATEWAY 6102 & CARRIED OUT

S6603

ESTABLISH ISOCHRONOUS CHANNEL #x ON 1394 BUS
USING AV/C PROTOCOL, & RECEIVE COMMAND
"CONNECT THIS TO VIDEO TRANSMISSION SUB-UNIT"
FROM HOME GATEWAY

S6604

TRANSMIT ENCRYPTED MPEG2 VIDEO TO
ISOCHRONOUS CHANNEL #x (CONTENTS KEY=K1)

S6605

RECEIVE AUTHENTICATION TARGET QUERY FROM
(MPEG DECODING/DISPLAY SUB-UNIT OF)
HOME GATEWAY

S6606

SEARCH TRANSMISSION SUB-UNIT OF CHANNEL #x &
RETURN "AUTHENTICATION TARGET IS VIDEO
TRANSMISSION SUB-UNIT" AS AUTHENTICATION
TARGET REPLY TO HOME GATEWAY

S6607

RECEIVE AUTHENTICATION REQUEST FOR VIDEO
TRANSMISSION SUB-UNIT

S6608

OBTAIN B'S AUTHENTICATION FORMAT
(DEVICE CERTIFICATE) (Bcert)

R22

FIG.47

(R22)

S6609

SEND OWN AUTHENTICATION FORMAT
(DEVICE CERTIFICATE) Acert, ETC.
(OF VIDEO TRANSMISSION SUB-UNIT) AS
AUTHENTICATION REQUEST, TO MPEG
DECODING/DISPLAY SUB-UNIT OF HOME GATEWAY

S6610

AUTHENTICATION & KEY EXCHANGE PROCEDURE
(CALCULATE AUTHENTICATE KEY Kauth1)

S6611

TRANSFER EXCHANGE KEY & SEED TO HOME
GATEWAY

S6612

ENCRYPT MPEG VIDEO BY USING CONTENTS KEY K1

S6613

SEND ENCRYPTED MPEG2 VIDEO THROUGH
ISOCHRONOUS CHANNEL #x

48/68

FIG.48

START

S6701
RECOGNIZE TRANSMISSION NODE CONFIGURATION INFORMATION BY READING IEEE1212 REGISTER OF TRANSMISSION NODE (RECOGNIZE THAT TRANSMISSION NODE HAS AUTHENTICATION FORMAT)

S6702
READ PANEL SUB-UNIT OF TRANSMISSION NODE

S6703
CREATE CONTROL DISPLAY FOR REMOTE CONTROL OF TRANSMISSION NODE ON HOME PAGE ACCORDING TO PANEL INFORMATION, RECORD CORRESPONDENCE IN CONVERSION TABLE & DISCLOSE IT TO INTERNET SIDE

S6704
RECEIVE OPERATION ON HOME PAGE FROM RECEPTION NODE VIA INTERNET
(e.g. A BUTTON INDICATING PLAYBACK IS PRESSED)

S6705
CARRY OUT SESSION CONTROL & DECIDE THAT MPEG DATA TRANSFER WILL BE CARRIED OUT BY USING FLOW (C,c,D,d)

S6706
SET UP ISOCHRONOUS CHANNEL #x & REQUEST VIDEO TRANSMISSION, ETC. BY USING AV/C PROTOCOL, WITH RESPECT TO TRANSMISSION NODE

S6707
RECEIVE DATA TRANSMITTED FROM TRANSMISSION NODE THROUGH ISOCHRONOUS CHANNEL #x & RECOGNIZE THAT IT IS ENCRYPTED DATA

R13

FIG.49

(R13)

S6708

SEND AUTHENTICATION TARGET QUERY TO TRANSMISSION NODE THAT IS SOURCE OF DATA IN ORDER TO INQUIRE TRANSMISSION SUB-UNIT.
(ALSO NOTIFY THAT RECEIVING SUB-UNIT IS MPEG DECODING/DISPLAY SUB-UNIT AT THE SAME TIME.)
ALSO SEND ISOCHRONOUS CHANNEL NUMBER #x

S6709

RECEIVE AUTHENTICATION TARGET REPLY FROM TRANSMISSION NODE. THE FACT THAT TRANSMISSION SUB-UNIT IS VIDEO TRANSMISSION SUB-UNIT IS ASCERTAINED

S6710

SEND AUTHENTICATION REQUEST TO VIDEO TRANSMISSION SUB-UNIT OF TRANSMISSION NODE (ALSO SEND AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Bcert OF MPEG DECODING / DISPLAY SUB-UNIT)

S6711

RECEIVE AUTHENTICATION REQUEST FOR MPEG DECODING/DISPLAY SUB-UNIT

S6712

OBTAIN AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Acert OF VIDEO TRANSMISSION SUB-UNIT OF TRANSMISSION NODE

S6713

AUTHENTICATION & KEY EXCHANGE PROCEDURE (CALCULATE AUTHENTICATION KEY Kauth1)

S6714

RECEIVE EXCHANGE KEY & SEED FROM TRANSMISSION NODE

S6715

CALCULATE CONTENTS KEY K1

(R23)

50/68

FIG.50

R23

S6716
RECEIVE ENCRYPTED MPEG2 VIDEO THROUGH ISOCHRONOUS CHANNEL #x & DECRYPT IT

S6717
DECODE MPEG2 & RE-ENCODE AS MPEG4

S6718
RE-ENCRYPT MPEG4 DATA BY USING CONTENTS KEY K2

S6719
SEND ENCRYPTED MPEG4 VIDEO TO RECEPTION NODE BY USING IP PACKET WITH FLOW ID=(C,c,D,d)

S6720
RECEIVE AUTHENTICATION REQUEST FOR FLOW ID=(C,c,D,d)

S6721
OBTAIN D'S AUTHENTICATION FORMAT (DEVICE CERTIFICATE) (Dcert)

S6722
SEND AUTHENTICATION FORMAT Ccert, ETC. AS AUTHENTICATION REQUEST FOR FLOW ID=(C,c,D,d) TO RECEPTION NODE

S6723
AUTHENTICATION & KEY EXCHANGE PROCEDURE (CALCULATE AUTHENTICATION KEY Kauth2)

R24

FIG.51

R24

S6724

TRANSFER EXCHANGE KEY & SEED TO RECEPTION NODE

S6725

ENCRYPT MPEG4 VIDEO BY USING CONTENTS KEY K2

S6726

SEND ENCRYPTED MPEG4 VIDEO TO RECEPTION NODE BY USING IP PACKET WITH FLOW ID=(C,c,D,d)

FIG.52

START

S6801

HOME PAGE FOR REMOTE CONTROL OF TRANSMISSION NODE IS RECEIVED

S6802

RECEPTION NODE USER PRESSES BUTTON FOR "REQUEST VIDEO TRANSMISSION" FOR HOME GATEWAY SO THAT PRESSING OF THAT BUTTON IS NOTIFIED TO HOME GATEWAY BY HTTP

S6803

CARRY OUT SESSION CONTROL & DECIDE THAT MPEG DATA TRANSFER WILL BE CARRIED OUT BY USING FLOW (C,c,D,d)

S6804

RECEIVE ENCRYPTED MPEG4 VIDEO USING IP PACKET WITH FLOW ID=(C,c,D,d)

S6805

SEND OWN AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Dcert, ETC. AS AUTHENTICATION REQUEST FOR FLOW WITH FLOW ID=(C,c,D,d) TO HOME GATEWAY

S6806

RECEIVE AUTHENTICATION REQUEST FOR FLOW ID=(C,c,D,d) FROM HOME GATEWAY

S6807

OBTAIN C'S AUTHENTICATION FORMAT (DEVICE CERTIFICATE) (Ccert)

S6808

AUTHENTICATION & KEY EXCHANGE PROCEDURE (CALCULATE AUTHENTICATION KEY Kauth2)

R25

FIG.53

R25

S6809
EXCHANGE KEY & SEED ARE RECEIVED FROM HOME GATEWAY

S6810
GENERATE CONTENTS KEY K2

S6811
SEND ENCRYPTED MPEG4 VIDEO TO RECEPTION NODE BY USING IP PACKET WITH FLOW ID=(C,c,D,d)

S6812
DECRYPT IT BY USING CONTENTS KEY K2 & DECODE MPEG4

S6813
DISPLAY AT DISPLAY UNIT

FIG.54

(b)

HOME PAGE FOR
TRANSMISSION NODE CONTROL

VTR CONTROL PAGE

| REVERSE | STOP | PLAYBACK | FAST FORWARD |

PRODUCED IN
SIMILAR
CONFIGURATION
AS MUCH AS
POSSIBLE

⇧

(a)

PANEL AT PANEL SUB-UNIT
OF TRANSMISSION NODE

VTR CONTROL DISPLAY

| REVERSE | STOP | PLAYBACK | FAST FORWARD |

55/68

FIG.55

RADIO NODE   9103

9102   RADIO SECTION

RELAY NODE

9101   TRANSMISSION NODE

IEEE1394 BUS   9104

FIG.56

```
                                          ┌─────────────────┐ ～9404
                                          │     MPEG        │
                                          │  STORAGE UNIT   │
                                          └────────┬────────┘
                         ～9403                     │ MPEG VIDEO
┌──────────────────────────────┐                  ▼        ～9405
│ COPY PROTECTION              │         ┌─────────────────┐
│ PROCESSING UNIT              │  KEY K  │ ENCRYPTION UNIT │
│ ┌──────────────────────────┐│────────▶│                 │
│ │ AUTHENTICATION           ││         └────────┬────────┘
│ │ FORMAT (DEVICE           ││                  │ [MPEG VIDEO]K
│ │ CERTIFICATE)  Acert      ││                  ▼        ～9406
│ └──────────────────────────┘│         ┌─────────────────┐
└───────────────┬──────────────┘         │ ISO SIGNAL      │
                │            ～9402        │ TRANSMISSION &  │
┌───────────────┴──────────────┐         │ RECEPTION UNIT  │
│ AV/C PROTOCOL                │         └────────┬────────┘
│ PROCESSING UNIT              │                  │        ～9401
└───────────────┬──────────────┘                  ▼
                │                                   │
┌───────────────┴──────────────────────────────────┴────────┐
│                    IEEE1394 I/F                            │
└────────────────────────────────────────────────────────────┘
```

FIG.57

FIG.58

9307

DISPLAY UNIT

↑ VIDEO

9306

MPEG DECODING
UNIT

↑ MPEG VIDEO

9303

COPY PROTECTION
PROCESSING UNIT

AUTHENTICATION
FORMAT (DEVICE
CERTIFICATE) Dcert

KEY K →

9305

DECRYPTION UNIT

↑ [MPEG VIDEO]K

9302

RADIO NODE
CONTROL PACKET
TRANSMISSION &
RECEPTION UNIT

9304

RADIO ISO SIGNAL
TRANSMISSION &
RECEPTION UNIT

9301

RADIO I/F

FIG.59

TRANSMISSION NODE 9101   RELAY NODE 9102   RADIO NODE 9103

[MPEG VIDEO]K(VIA #x) — S8501

[MPEG VIDEO]K(VIA #y) — S8509

AUTHENTICATION REQUEST
TO:TRANSMISSION NODE, Bcert — S8502

AUTHENTICATION REQUEST
TO:RELAY NODE, Dcert — S8510

AUTHENTICATION REQUEST
TO:RELAY NODE, Acert — S8503

AUTHENTICATION REQUEST
TO:RADIO NODE, Ccert — S8511

AUTHENTICATION
& KEY EXCHANGE PROCEDURE — S8504

AUTHENTICATION
& KEY EXCHANGE PROCEDURE — S8512

Kauth1
SHARING

Kauth1
SHARING — S8505

Kauth2
SHARING — S8513

Kauth2
SHARING — S8514

f(Kx, Kauth1) — S8506

Kx
SHARING

f(Kx, Kauth2)

SEED Nc TRANSFER — S8507

Nc

Nc

SEED Nc TRANSFER — S8515

[MPEG VIDEO]K(VIA #x) — S8508

[MPEG VIDEO]K(VIA #y) — S8517

CALCULATION
OF K — S8516

DECRYPTION
& DECODING — S8518

60/68

FIG.60

START

S8601

SEND MPEG VIDEO ENCRYPTED BY USING CONTENTS KEY K TO ISOCHRONOUS CHANNEL #x

S8602

RECEIVE AUTHENTICATION REQUEST (CONTAINING AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Bcert OF RELAY NODE) FROM RELAY NODE

S8603

TRANSMIT AUTHENTICATION REQUEST (CONTAINING AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Acert OF TRANSMISSION NODE) TO RELAY NODE

S8604

CARRY OUT AUTHENTICATION & KEY EXCHANGE PROCEDURE TO SHARE AUTHENTICATION KEY Kauth1 WITH RELAY NODE

S8605

TRANSMIT EXCHANGE KEY Kx TO RELAY NODE (IN FORM FUNCTION f(Kx, Kauth1))

S8606

TRANSMIT SEED Nc TO RELAY NODE

S8607

SEND MPEG DATA ENCRYPTED BY USING CONTENTS KEY K TO ISOCHRONOUS CHANNEL #x

FIG.61

START

S8701

RECEIVE MPEG VIDEO ENCRYPTED BY USING CONTENTS KEY K FROM ISOCHRONOUS CHANNEL #x OF IEEE1394 & RECOGNIZE THAT IT IS ENCRYPTED DATA TRANSMITTED FROM TRANSMISSION NODE. TRANSMIT IT TO RADIO ISOCHRONOUS CHANNEL #y OF RADIO NETWORK AS IT IS WITHOUT CARRYING OUT DECRYPTION, ETC.

S8702

TRANSMIT AUTHENTICATION REQUEST (CONTAINING IEEE1394 SIDE AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Bcert OF RELAY NODE) TO TRANSMISSION NODE

S8703

RECEIVE AUTHENTICATION REQUEST (CONTAINING AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Acert OF TRANSMISSION NODE) FROM TRANSMISSION NODE

S8704

CARRY OUT AUTHENTICATION & KEY EXCHANGE PROCEDURE TO SHARE AUTHENTICATION KEY Kauth1 WITH TRANSMISSION NODE

S8705

RECEIVE AUTHENTICATION REQUEST (CONTAINING AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Dcert OF RADIO NODE) FROM RADIO NODE

R26

62/68

FIG.62

(R26)

S8706

TRANSMIT AUTHENTICATION REQUEST (CONTAINING RADIO NETWORK SIDE AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Ccert OF RELAY NODE) TO RADIO NODE

S8707

CARRY OUT AUTHENTICATION & KEY EXCHANGE PROCEDURE TO SHARE AUTHENTICATION KEY Kauth2 WITH RADIO NODE

S8708

RECEIVE EXCHANGE KEY Kx FROM TRANSMISSION NODE (IN FORM OF FUNCTION f(Kx, Kauth1))

S8709

EXTRACT EXCHANGE KEY Kx & TRANSMIT EXCHANGE KEY Kx TO RADIO NODE (IN FORM OF FUNCTION f(Kx, Kauth2))

S8710

RECEIVE SEED Nc FROM TRANSMISSION NODE

S8711

TRANSMIT SEED Nc TO RADIO NODE

S8712

RECEIVE MPEG VIDEO ENCRYPTED BY USING CONTENTS KEY K FROM ISOCHRONOUS CHANNEL #x OF IEEE1394 & TRANSMIT IT TO RADIO ISOCHRONOUS CHANNEL #y OF RADIO NETWORK AS IT IS WITHOUT CARRYING OUT DECRYPTION, ETC.

FIG.63

START

S8801

RECEIVE MPEG VIDEO ENCRYPTED BY USING CONTENTS KEY K FROM RADIO ISOCHRONOUS CHANNEL #y & RECOGNIZE THAT IT IS ENCRYPTED DATA TRANSMITTED FROM RELAY NODE

S8802

TRANSMIT AUTHENTICATION REQUEST (CONTAINING AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Dcert OF RADIO NODE) TO RELAY NODE

S8803

RECEIVE AUTHENTICATION REQUEST (CONTAINING AUTHENTICATION FORMAT (DEVICE CERTIFICATE) Ccert OF RELAY NODE) FROM RELAY NODE

S8804

CARRY OUT AUTHENTICATION & KEY EXCHANGE PROCEDURE TO SHARE AUTHENTICATION KEY Kauth2 WITH RELAY NODE

S8805

RECEIVE EXCHANGE KEY Kx FROM RELAY NODE (IN FORM OF FUNCTION f(Kx, Kauth2))

S8806

EXTRACT EXCHANGE KEY Kx

R27

FIG.64

R27

S8807

RECEIVE SEED Nc FROM RELAY NODE

S8808

CALCULATE CONTENTS KEY K

S8809

RECEIVE MPEG VIDEO ENCRYPTED BY USING CONTENTS KEY K FROM RADIO ISOCHRONOUS CHANNEL #y

S8810

DECRYPT IT BY USING CONTENTS KEY K & DECODE IT

FIG.65

RADIO NODE — 9803

RADIO SECTION

RELAY NODE — 9802

TRANSMISSION NODE Q — 9811

TRANSMISSION NODE P — 9801

IEEE1394 BUS — 9804

FIG.66

```
( START )
```

⤵ S9201

RECEIVE MPEG VIDEO ENCRYPTED BY USING
CONTENTS KEY K1 FROM ISOCHRONOUS CHANNEL #x
OF IEEE1394 & RECOGNIZE THAT IT IS ENCRYPTED
DATA TRANSMITTED FROM TRANSMISSION NODE P.
TRANSMIT IT TO RADIO ISOCHRONOUS CHANNEL #y
OF RADIO NETWORK AS IT IS WITHOUT CARRYING
OUT DECRYPTION, ETC.

⤵ S9202

CARRY OUT AUTHENTICATION & KEY EXCHANGE
WITH TRANSMISSION NODE P & ACQUIRE EXCHANGE
KEY Kxp & SEED Ncp

⤵ S9203

CARRY OUT AUTHENTICATION & KEY EXCHANGE IN
UNITS OF SUB-UNITS (FUNCTIONS) WITH RADIO NODE
& SEND EXCHANGE KEY Kxp & SEED Ncp

⤵ S9204

RECEIVE MPEG VIDEO ENCRYPTED BY USING
CONTENTS KEY K2 FROM ISOCHRONOUS CHANNEL #x'
OF IEEE1394 & RECOGNIZE THAT IT IS ENCRYPTED
DATA TRANSMITTED FROM TRANSMISSION NODE Q.
TRANSMIT IT TO RADIO ISOCHRONOUS CHANNEL #z
OF RADIO NETWORK AS IT IS WITHOUT CARRYING
OUT DECRYPTION, ETC.

⤵ S9205

CARRY OUT AUTHENTICATION & KEY EXCHANGE
WITH TRANSMISSION NODE Q & ACQUIRE EXCHANGE
KEY Kxq & SEED Ncq

⤵ S9206

CARRY OUT AUTHENTICATION & KEY EXCHANGE IN
UNITS OF SUB-UNITS (FUNCTIONS) WITH RADIO NODE
& SEND EXCHANGE KEY Kxq & SEED Ncq

FIG.67

TRANSMISSION NODE P 9801

TRANSMISSION NODE Q 9811

RELAY NODE 9802

RADIO NODE 9803

[MPEG VIDEO]K1 (VIA #x) — S9201

[MPEG VIDEO]K1 (VIA #y) — S9209

AUTHENTICATION REQUEST TO:TRANSMISSION NODE P,Bcert — S9202

AUTHENTICATION TARGET QUERY FROM;RADIO NODE,(VIDEO DECODING SUB-UNIT, ID=0) OR iPCR[0], (CH=#y) — S9210

AUTHENTICATION REQUEST TO:RELAY NODE,Pcert,Bdid — S9203

AUTHENTICATION TARGET REPLY FROM;RELAY NODE,(VIDEO TRANSMISSION SUB-UNIT, ID=0) OR oPCR[0], (CH=#y) — S9211

AUTHENTICATION & KEY EXCHANGE PROCEDURE — S9205

AUTHENTICATION REQUEST TO:RELAY NODE,(VIDEO TRANSMISSION SUB-UNIT:ID=0) OR oPCR[0] OR #y, Dcert — S9212

S9204 — KauthP SHARING

KauthP SHARING

AUTHENTICATION REQUEST TO:RADIO NODE,(VIDEO DECODING SUB-UNIT:ID=0) OR iPCR[0] OR #y, Dcert, Ddid — S9213

f(Kxp, KauthP) — SEED:Ncp TRANSFER — S9206

AUTHENTICATION & KEY EXCHANGE PROCEDURE — S9214

kxp — S9207

Kauth1 SHARING

Kauth1 SHARING — S9215

[MPEG VIDEO]K1(VIA #x) — S9208

Ncp — SUB-UNIT ID OR PLUG ID OR #y f(Kxp, Kauth1) — S9216

SEED:Ncp TRANSFER — S9217

kxp — S9218

Ncp — CALCULATION OF K1

[MPEG VIDEO]K1(VIA #y) — S9219

S9220 — DECRYPTION & DECODING

FIG.68

TRANSMISSION NODE P 9801

TRANSMISSION NODE Q 9811

RELAY NODE 9802

RADIO NODE 9803

[MPEG VIDEO]K2 (VIA #x') — S9221

[MPEG VIDEO]K2 (VIA#z) — S9229

AUTHENTICATION REQUEST TO:TRANSMISSION NODE Q, Bcert — S9222

AUTHENTICATION TARGET QUERY FROM;RADIO NODE,(VIDEO DECODING SUB-UNIT, ID=1) OR iPCR[1], (CH=#z) — S9230

AUTHENTICATION REQUEST TO:RELAY NODE, Qcert, Bdid — S9223

AUTHENTICATION TARGET REPLY FROM;RELAY NODE,(VIDEO TRANSMISSION SUB-UNIT, ID=1) OR oPCR[1], (CH=#z) — S9231

AUTHENTICATION & KEY EXCHANGE PROCEDURE — S9224

KauthQ SHARING — S9225

AUTHENTICATION REQUEST TO:RELAY NODE,(VIDEO TRANSMISSION SUB-UNIT, ID=1) OR oPCR[1] OR #z, Dcert — S9232

KauthQ SHARING

f(Kxq, KauthQ) — S9226

AUTHENTICATION REQUEST TO:RADIO NODE,(VIDEO DECODING SUB-UNIT: ID=1) OR #z, Ccert, Ddid — S9233

SEED Ncq TRANSFER — S9227

kxq

AUTHENTICATION & KEY EXCHANGE PROCEDURE — S9234

[MPEG VIDEO]K2(VIA #x') — S9228

Ncq — S9235

Kauth2

SHARING SUB-UNIT ID OR PLUG ID OR #z — S9236

Kauth2 SHARING

f(Kxq, Kauth2)

SEED Ncp TRANSFER — S9237

kxq — S9238

[MPEG VIDEO]K2(VIA #z) — S9239

Ncq

CALCULATION OF K2

DECRYPTION & DECODING — S9240